

EXHIBIT 8



Part of the **TechWeb** Business Technology Network

Save money and re
Management: Do

systemsmanagementpi

SEARCH search advanced search

Free Newsletter Glossary Contact Us

NEWS | TRENDS | HANDS ON | BLOG | PRODUCT FINDER | HARDWARE | SOFTWARE | NETWORK | L

how-to

December 03, 2004

Review: Network Forensic Tools

Stage 1: From a Distance

By Marisa Mack

Courtesy of Network Computing

Page 2 of 6

A first responder—the first person to identify and access a system involved in an incident—must be aware of the importance of preserving evidence. Under no circumstances should a first responder modify, delete or change data on the evidentiary system. This is where the network-capable features of the products we tested are valuable. Note: All product write-ups are listed alphabetically. Our features chart on page 50 gives a summary of each product's capabilities.

Guidance Software EnCase Enterprise Edition 4.19

Any investigation begins with discovery and analysis of the incident. EnCase Enterprise Edition can do both: Guidance markets its enterprise product as an intrusion-detection system as well as an incident-response tool. EnCase Enterprise monitored the known-good state of our networked clients and automatically created a preview image of any system that changed from its established state. This was all done through hash verification of files installed on the network clients. Additionally, we could configure EnCase Enterprise to remove any suspicious services or programs on client machines automatically.

On the surface, having one application that both detects and responds to an incident makes sense. However, we think Guidance should separate the product into two offerings—one for IDS and one for response—or simply remove the incident-detection features and lower the price.

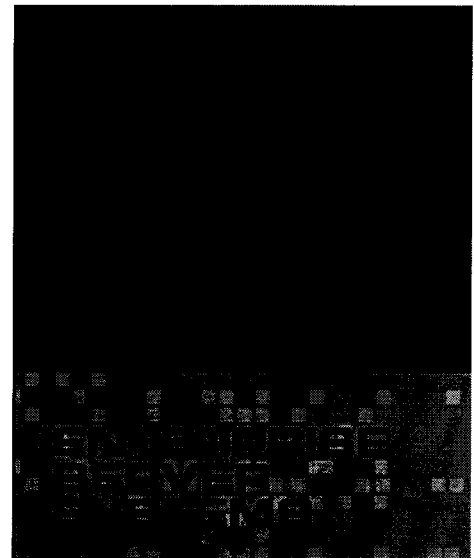
EnCase Enterprise Edition's as-tested cost includes one EnCase Examiner installation, the SAFE (Secure Authentication For EnCase) authentication server and an unlimited number of installed client servlets. It's a significant investment for organizations unsure of their forensic needs. The extra functionality is useful, but it would be better to have the option to acquire drive images remotely without the big price increase from Guidance's Forensic Edition product. While EnCase muddled the water by marketing its product as an IDS, it's still the single most useful application for investigators.

If cost is not a huge concern, there's a lot to love about this product. Any EnCase Enterprise installation is helped along by a dedicated Guidance

RELATED LINKS

- ☐ [Bagle Bullies Users Into Infections](#)
- ☐ [PC-To-Mobile Trojan Mystery Puzzles](#)
- ☐ [Oracle Patches E-Business Security | Schedule](#)
- ☐ [Adware Firm 180Solutions Apologize](#)
- ☐ [Gaming, Celebrity Sites Nastiest Web](#)
- ☐ [Critical Shockwave Install Bug Fixed](#)

RSS [Systems Management Pipeline's Ma](#)
RSS [Systems Management Pipeline's Bl](#)



SMB How-To Guide On Setting Up
Follow these easy steps written just for the understanding and implementing WLAN te

How to Achieve High Performance
Learn to achieve high performance by align strategic objectives and solutions to unlock

Using Current Performance to Sh: Future Results
Hear new strategies for improving business performance and results..

Software sales engineer. Configured as directed, the EnCase client servlet should be installed on all the client machines on your network. This is a huge administrative task for an established enterprise-level network, but the functionality offered by this configuration will reduce time lost to frequent anomaly investigations.

The EnCase SAFE authentication server manages user and group access to any beginning or ongoing investigation. Before opening any case or communicating with installed client servlets, users must provide login credentials to the SAFE server over a 128-bit AES connection. Authentication is based on a public-key cryptosystem, using public and private key verification between the SAFE server and the investigator.

Configuring user roles and privileges wasn't difficult. We could assign role-based permissions to users or groups to access individual clients or ranges of client addresses. For our tests, we created both a primary investigator user as well as an assistant user with lesser privileges to access clients on our test network. In this environment, Encase Enterprise detected the KeySnatch Trojan running on one of our clients and automatically provided a preview of the infected drive. As configured, our assistant user could assess the drive preview to verify the findings, while only the primary user could delete the Trojan file. In an actual incident, this role separation allows more granularity in responsibility and response, which can reduce the time and interruption caused by initial investigation.

By previewing the system, we could perform cursory investigation or navigation of a remote drive without creating an entire drive image, as if we had mounted the entire remote drive as a network share. All services and processes running on the remote machine can be viewed and assessed. We detected and removed a Trojan servlet running on the client machine, though EnCase Enterprise can be configured to remove this type of file automatically upon discovery. The documentation is complete and mature, but we wish it were available under the help menu—an expected standard for most applications. Beyond the networking functionality, EnCase Enterprise has the same interface and feature set as the less-expensive Forensic Edition.

*EnCase Enterprise Edition 4.19. Guidance Software, (626) 229-9191.
www.guidancesoftware.com*

Technology Pathways ProDiscover Incident Response 3.2

ProDiscover is a better choice for small and midsize businesses, mainly because of its \$2,995 price, which includes one concurrent user on as many as three installed machines and an unlimited number of client agent installs. Our installation included the ProDiscover Investigator interface running on a Windows XP system, connecting to a remote client agent installed on a Windows 2000 Professional machine. We acquired images of the remote drive over a 100-Mbps LAN used only for this test.

ProDiscover can image a system remotely in proprietary mode or in "dd" format, which can be read by any forensic tool later in the investigation. We used the "dd" format most of the time so that the created images could be read by additional investigative tools. The ProDiscover interface is less daunting than the EnCase interface, because it simply does less—only what's needed for initial analysis of an affected system. Our biggest concern was a persistent network time-out we obtained initially in testing on the Windows XP platform; luckily, the release notes contained instructions on how to fix this. The company says an updated version of ProDiscover (3.5) will fix the problem and add significant functionality (it was released just as we were completing this article).

Network client machines don't have the ProDiscover client agent up and running continuously as an additional network service, so initial investigation

TECHWEBCASTS

Editorial and vendor perspectives
SQL Server 2005 finally unleashed, get the facts on what's new..
Server virtualization cuts costs, boosts reliability. Take the next step..

VENDOR RESOURCES

Align IT with business: Adopt ITIL. Free white paper tells you how!
Download a free Architect's Guide on Data Center cooling solutions..

FOCAL POINTS

(Sponsored links)

Blade servers: Bigger isn't always better.
SOA lets government agencies make better use of legacy systems..

EDITOR'S PICKS

Firefox: How To Find And Use Your Protection

System administrators, it is time to come up t essentials. Here is a guideline on how to find what types of files you'll find there, and how y them against mishaps.

Far Too Many Phishing Expeditions Hit Users

Yahoo Battles Many Challenges

Five Things You Didn't Know (But Sho Core Processors

Is Google Desktop Too Risky For Your

VOTING BOOTH

Are you satisfied with what your company with computer hardware at the end of the equipment's lifecycle?

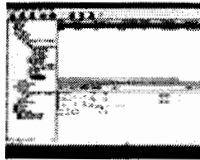
- ☐ Yes - we donate used hardware to scl and/or the underprivileged where I am sui used well.
- ☐ Mixed feelings - our policies are very inconsistent. We sometimes donate the hardware but sometimes we just dump it.
- ☐ Negative on our policy - we donate an dump hardware before it should be retirec processing it is a pain.
- ☐ Very negative on our policies - the reti hardware ends up in a landfill, where it ca anyone.

Vote

product find

Looking for systems management solutions Product Finder, an extensive directory of to applications, hardware, patches, backup, p scheduling, virtualization, and more.

requires that the ProDiscover client CD be introduced to the suspect machine. ProDiscover comes with batch-file scripts to push the agent onto a target machine—but this will modify the drive contents of the machine in question. Because the client agent can run as a service on Windows machines, it's feasible to have it running on all your intranet clients, as EnCase Enterprise does. However, we wish Technology Pathways would address this specific scenario clearly in its documentation, as modifying a target during investigation is forensically unacceptable. Throughout our tests, we had no problems keeping the client agents running on all our network clients, which let us obtain previews of existing clients without modification.



ProDiscover
[Click to Enlarge](#)

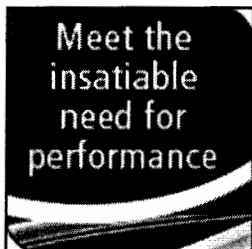
The filtering and scripting functions aren't as useful or robust as those in the EnCase suite; however, remotely acquiring an image worked to forensic standards, and we could open that image for analysis in a separate application. ProDiscover doesn't feel like it's undergone the same level of quality assurance as EnCase. For example, error messages are sometimes poorly written, and one of the dialog menus contains a misspelling, though none of these flaws prevented a complete product analysis.


ProDiscover Incident Response 3.2. Technology Pathways, (888) 894-5500, (619) 435-0906. www.prodiscover.com

[E-mail This Story](#)
[Print This Story](#)
[Reprint This Story](#)

Page 3: Stage 2: The Right Hand

[Page 1](#) | [2](#) | [3](#) | [4](#) | [5](#) | [6](#)



FREE SYS MANAGEMENT
 NEWSLETTER 
 Get the latest Systems
 Management news, product info,
 and trends every week.

Subscribe!

SYSTEMS MANAGEMENT PIPELINE MARKETPLACE (sponsored links)

Disaster Recovery Seminar

Network with other Symantec Users. Discuss Ideas and Share Solutions!

Want to know your CIS security score?

The CIS has developed detailed IT security benchmarks which will help make your computer more secure. Click here to download the Belarc Advisor which will automatically show you how secure your system is compared the CIS benchmark configurations.

Security Within - Configuration based Security

Configuration and policy based security systems are a pro-active way to defend against IT security attacks. Click here to request our white papers, "Security Within - Configuration based Security" and "Policy Management vs. Vulnerability Scanning".

Authentication TCO White Paper from VeriSign

Discover how to secure multiple devices across your enterprise, plus reduce TCO and complexity by implementing a two-factor unified authentication solution. Leverage your existing infrastructure. Learn more.

Industry Leading - Security Patch Management

Automated Security Patch Management protects from Internet Worms and security issues. Your team will be

patching in 30 minutes. Free Trial Version has no time-out. Most cost effective security solution available, Powered by Shavlik HFNetChkPro.

Buy a Link Now

Hewlett-Packard Back up your important business data with the HP DAT 72 USB tape drive..
How does your pay rate? Check the InformationWeek Salary Survey.
Mobilized Solutions Guide: Find and compare solutions for your business.
Top Requested White Paper Categories from TechWeb White paper Library.
Top ten search terms from the TechWeb TechEncyclopedia.

Sponsored Links: [Save money and reduce risk with IT Asset Management: Download the white paper.](#) [Sponsor Resources.](#) [We](#)

News | Trends | Product Finder | Hands On | Blog | Hardware | Software | Network | Lifecycle & Original Articles | Free Newsletters | Systems Management Glossary | Contact Us | About Us | Priva

[The TechWeb Pipelines](#) | [TechWeb.com](#) | [InformationWeek](#) | [Optimize](#) | [Network Computing](#) | [IT Architect](#) | [Intelligen](#)
[Bank Systems & Technology](#) | [Wall Street & Technology](#) | [Insurance & Technology](#) | [IT Pro Downloads](#) | [Comm](#)
[Business Intelligence Pipeline](#) | [Compliance Pipeline](#) | [Desktop Pipeline](#) | [Developer Pipeline](#) | [InternetWeek](#) | [Linux](#)
[Messaging Pipeline](#) | [Networking Pipeline](#) | [Personal Tech Pipeline](#) | [Security Pipeline](#) | [Server Pipeline](#)
[Small Business Pipeline](#) | [SOA Pipeline](#) | [Systems Management Pipeline](#) | [Byte and Switch](#) | [Light Reading](#) | [Un](#)

Copyright © 2006 CMP Media LLC. | SYSTEMS MANAGEMENT PIPELINE All rights reserved. [Privacy Policy](#) | [Your California Privacy Rights](#) | [Terms](#)